

Remark

Applicant respectfully requests reconsideration of this application as amended. No Claims have been amended. No Claims have been cancelled. Therefore, claims 1-21 are present for examination.

35 U.S.C. §103 Rejection*Kamiya in view of Menezes*

The Examiner has rejected claims 1-21 under 35 U.S.C. §103 (a) as being unpatentable over Kamiya et al., U.S. Publication No. US 2002/0106086 A1 ("Kamiya"), in view of Menezes et al., Menezes, Handbook of Applied Cryptography, ("Menezes"). The Examiner acknowledges that Kamiya does not show many of the encryption functions of the present invention and relies on Menezes for that purpose.

Menezes does not teach "simultaneously decrypting and re-encrypting" (Claim 1) nor any operations involving video or "encrypted video" (Claim 1). Menezes also does not teach using "a combination of the first and the second cipher streams" (Claim 1). However, even assuming for the sake of argument, that Menezes teaches all that the Examiner suggests, the combination is still insufficient to render the pending claims obvious.

First, MPEP 2143.01 (V.) requires that a proposed modification of a prior art reference may not be used to reject a claim if the modification would render the reference unsatisfactory for its intended purpose. In Kamiya Figure 4, for example, between the decryption unit and the scramble unit, there is a decoding unit 35C. In the Kamiya system, as explained in paragraph 0079, the video arrives encoded using an MPEG or

similar coder. The decoding can only be done when the video is in the clear. The decryption section 35 must therefore decrypt before decoding and then encrypt after decoding. To decrypt and encrypt simultaneously would render the decoder inoperative.

Second, the MPEP requires that the prior art must suggest the desirability of the claimed invention (MPEP 2143.01(I)). The suggestion may be explicit or implicit. The Examiner states that the references are combinable based on a motivation to "prevent data from being intercepted during decryption and re-encryption process when data is in the clear." Applicants are unable to find any suggestion, whether explicit or implicit of such a motivation in Menezes, nor in Kamiya.

Such a motivation is provided by the present application as stated in paragraph 28. "As discussed above, the unique trusted module makes it possible to decrypt and re-encrypt a digital stream in one step using an exclusive-OR operation based on the two keys. As a result, the content is never in the clear, i.e. it is never present in a decrypted form. This greatly enhances the total security of the system."

For a proper rejection, however, the motivation must come from the prior art, not the pending application. MPEP 2143.01 suggests if there is no suggestion in the references (and there is not), then the combined teachings, knowledge of one of ordinary skill and the nature of the problem as a whole must suggest the combination.

The teachings of Kamiya are to provide decryption and scrambling as two different processes with two different keys performed by different units. The keys are even generated in different places, one by a server and one locally. The teachings of Menezes are about encryption generally with no suggested applications of any kind. The only problem suggested is that of the key being broken. The complexity of the Kamiya

device shows that the problem to be solved in Kamiya is far more complex than simply avoiding the breaking of the keys. Ultimately, there must be content and that content must be provided to a user with a minimum of inconvenience and expense.

Conclusion

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims as amended be allowed.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.


Request for an Extension of Time

Applicant respectfully petitions for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17(a) for such an extension. Charge our Deposit Account.

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: April 20, 2006


Gordon R. Lindeen III
Reg. No. 33,192

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1030
(303) 740-1980